New Extremal Self-Dual Binary Codes of Length 68 via Composite Construction, $\mathbb{F}_2 + u\mathbb{F}_2$ Lifts, Extensions and Neighbors

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510
USA
prof.steven.dougherty@gmail.com
Joe Gildea, Adrian Korban
Department of Mathematical and Physical Sciences
University of Chester
Thornton Science Park, Pool Ln, Chester CH2 4NU, England
j.gildea@chester.ac.uk
adrian3@windowslive.com
Abidin Kaya
Department of Mathematics Education
Sampoerna University, 12780, Jakarta, Indonesia
abidin.kaya@sampoernauniversity.ac.id

February 29, 2020

Abstract

We describe a composite construction from group rings where the groups have orders 16 and 8. This construction is then applied to find the extremal binary self-dual codes with parameters $[32, 16, 8]$ or $[32, 16, 6]$. We also extend this composite construction by expanding the search field which enables us to find more extremal binary self-dual codes with the above parameters and with different orders of automorphism groups. These codes are then lifted to $\mathbb{F}_2 + u\mathbb{F}_2$, to obtain extremal binary images of

codes of length 64. Finally, we use the extension method and neighbor construction to obtain new extremal binary self-dual codes of length 68. As a result, we obtain 28 new codes of length 68 which were not known in the literature before.

Key Words: Group rings; self-dual codes; codes over rings.

1 Introduction

In this work, we combine different and well known techniques to find new extremal self-dual codes with parameters $[68, 34, 12]$. We start by considering the generator matrix of the form $(I_n|\sigma(v))$ where $\sigma(v)$ is the image of a unitary unit in a group ring under a map that sends group ring elements to matrices. We then extend the method described in [4], where the authors apply the map $\sigma(v)$ to different groups of orders 8 and 4 to get different block-matrices which they then combine together to form new matrices which can be used to search extremal binary self-dual codes. In our approach, we look at groups of orders 16 and 8. We describe a composite construction in the same way as in [4], which we then use over $\mathbb{F}_2$ to find extremal self-dual binary codes with parameters $[32, 16, 8]$ and $[32, 16, 6]$. We next lift these codes over $\mathbb{F}_2 + u\mathbb{F}_2$, to obtain the extremal binary images of self dual codes of length 64. We finally apply the extension and neighbors methods to find new extremal binary self-dual codes of length 68.

The rest of the work is organized as follows. In Section 2, we give preliminary definitions and results on group rings, self-dual codes and the alphabets which we use. In Section 3, we give the new composite construction which we then use to define the generator matrix which can be applied to find extremal binary self-dual codes. We also extend the generator matrix by extending the search field to enable us to find even more extremal self-dual binary codes with different orders of automorphism groups. In Section 4, we tabulate all the results from applying the generator matrices from the previous section to $\mathbb{F}_2 + u\mathbb{F}_2$. In Section 5, we find new extremal binary self-dual codes of length 68 by applying the extension and neighbors methods to the codes found in Section 4.

2 Preliminaries

2.1 Self-Dual Codes, the Ring $\mathbb{F}_2 + u\mathbb{F}_2$ and Group Rings

We begin by recalling the standard definitions from coding theory. A code C of length n over a Frobenius ring R is a subset of R^n. If the code is a submodule of R^n then we say that the code is linear. Elements of the code C are called codewords of C. Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ be two elements of R^n. The duality is understood in terms of the

Euclidean inner product, namely:

$$\langle \mathbf{x}, \mathbf{y} \rangle_E = \sum x_i y_i.$$

The dual $C^\perp$ of the code C is defined as

$$C^\perp = \{\mathbf{x} \in R^n \mid \langle \mathbf{x}, \mathbf{y} \rangle_E = 0 \text{ for all } \mathbf{y} \in C\}.$$

We say that C is self-orthogonal if $C \subseteq C^\perp$ and is self-dual if $C = C^\perp$.

An upper bound on the minimum Hamming distance of a binary self-dual code was given in [11]. Specifically, let $d_I(n)$ and $d_{II}(n)$ be the minimum distance of a Type I and Type II binary code of length n, respectively. Then

$$d_{II}(n) \leq 4\lfloor \frac{n}{24} \rfloor + 4$$

and

$$d_I(n) \leq \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4 & if\ n \not\equiv 22 \pmod{24} \\ 4\lfloor \frac{n}{24} \rfloor + 6 & if\ n \equiv 22 \pmod{24}. \end{cases}$$

Self-dual codes meeting these bounds are called *extremal*. Throughout the text, we obtain extremal binary codes of different lengths. Self-dual codes which are the best possible for a given set of parameters is said to be optimal. Extremal codes are necessarily optimal but optimal codes are not necessarily extremal.

2.2 The ring $\mathbb{F}_2 + u\mathbb{F}_2$

In this section, we recall some theory on self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. We refer to [2] where Type II, Type IV, self-dual codes and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ have been studied.

The ring $\mathbb{F}_2 + u\mathbb{F}_2$ is a ring of characteristic 2 with 4 elements with the restriction $u^2 = 0$. It is defined as

$$\mathbb{F}_2 + u\mathbb{F}_2 = \{a + bu \mid a, b \in \mathbb{F}_2, u^2 = 0\},$$

and it is easily seen that $\mathbb{F}_2 + u\mathbb{F}_2 \cong \mathbb{F}_2[x]/(x^2)$. A linear code C of length n over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ is an $\mathbb{F}_2 + u\mathbb{F}_2$-submodule of $(\mathbb{F}_2 + u\mathbb{F}_2)^n$. The elements of $\mathbb{F}_2 + u\mathbb{F}_2$ are $0, 1, u, 1+u$ and their Lee weights are defined as $0, 1, 2, 1$ respectively. The Hamming (d_H) and Lee (d_L) distance between n tuples is then defined as the sum of the Hamming and Lee weights of the difference of the components of these tuples respectively. The smallest positive Hamming and Lee distance of a code C is denoted by $d_H(C)$ and $d_L(C)$ respectively.

A Gray map ϕ is defined as

$$\phi : (\mathbb{F}_2 + u\mathbb{F}_2) \to \mathbb{F}_2^{2n},$$

$$\phi(\overline{a} + \overline{b}u) = (\overline{b}, \overline{a} + \overline{b}),$$

where $\overline{a}, \overline{b} \in \mathbb{F}_2^n$. The map is a distance preserving isometry from $((\mathbb{F}_2 + u\mathbb{F}_2)^n, d_L)$ to $(\mathbb{F}_2^{2n}, d_H)$, where d_L and d_H denote the Lee and Hamming distance in $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ and $\mathbb{F}_2^{2n}$ respectively. This means that if C is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ with parameters $[n, 2^k, d]$ (2^k is the number of the codewords), then $\phi(C)$ is a binary linear code of parameters $[2n, k, d]$. The following theorem is a natural result of the Gray map.

Theorem 2.1. *If C is a self-dual code over $\mathbb{F}_2 + u\mathbb{F}_2$ of length n, then $\phi(C)$ is a self-dual binary code of length $2n$.*

We can also define a natural projection from $\mathbb{F}_2 + u\mathbb{F}_2$ to $\mathbb{F}_2$ as follows:

$$\mu : \mathbb{F}_2 + u\mathbb{F}_2 \to \mathbb{F}_2,$$

$$\mu(a + bu) = a.$$

If $D = \mu(C)$ for some linear code C over $\mathbb{F}_2 + u\mathbb{F}_2$, we say that D is a projection of C into $\mathbb{F}_2$, and that C is a lift of D into $\mathbb{F}_2 + u\mathbb{F}_2$. It is clear that the projection of a self-orthogonal code is self-orthogonal, but the projection of a self-dual code need not be self-dual. We finish this section with two well known results.

Theorem 2.2. *Suppose that C is a self-dual code over $\mathbb{F}_2 + u\mathbb{F}_2$ of length $2n$, generated by the matrix $[I_n|A]$, where I_n is the $n \times n$ identity matrix. Then $\mu(C)$ is a self-dual binary code of length $2n$.*

Theorem 2.3. *Suppose C is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ and that $C' = \mu(C)$, is its projection to $\mathbb{F}_2$. With d and d' representing the minimum Lee and Hamming distances of C and C' respectively, we have that $d \leq 2d'$.*

2.3 Group Rings

To understand the composite construction which we define later in this work, we recall some basic definitions and theory on group rings and the map that sends group ring elements to matrices.

In our construction, we use circulant and block circulant matrices, both having the following form:

$$circ(\alpha_1, \alpha_2, \ldots, \alpha_n) = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \\ \alpha_n & \alpha_1 & \alpha_2 & \ldots & \alpha_{n-1} \\ \alpha_{n-1} & \alpha_n & \alpha_1 & \ldots & \alpha_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_2 & \alpha_3 & \alpha_4 & \ldots & \alpha_1 \end{pmatrix},$$

where $\alpha_i \in R$,

$$circ(A_1, A_2, \ldots, A_n) = \begin{pmatrix} A_1 & A_2 & A_3 & \ldots & A_n \\ A_n & A_1 & A_2 & \ldots & A_{n-1} \\ A_{n-1} & A_n & A_1 & \ldots & A_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & A_4 & \ldots & A_1 \end{pmatrix},$$

where each A_i is a $k \times k$ matrix over R, respectively. The transpose of a matrix A, denoted by A^T, is defined as $A^T_{ij} = A_{ji}$.

While group rings can be given for infinite rings and infinite groups, we are only concerned with group rings where both the ring and the group are finite. Let G be a finite group of order n, then the group ring RG consists of $\sum_{i=1}^{n} \alpha_i g_i$, $\alpha_i \in R$, $g_i \in G$.

Addition in the group ring is done by coordinate addition, namely

$$\sum_{i=1}^{n} \alpha_i g_i + \sum_{i=1}^{n} \beta_i g_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) g_i. \tag{1}$$

The product of two elements in a group ring is given by

$$\left(\sum_{i=1}^{n} \alpha_i g_i \right) \left(\sum_{j=1}^{n} \beta_j g_j \right) = \sum_{i,j} \alpha_i \beta_j g_i g_j. \tag{2}$$

It follows that the coefficient of g_i in the product is $\sum_{g_i g_j = g_k} \alpha_i \beta_j$.

The following construction of a matrix was first given for codes over fields by Hurley in [9]. It was extended to Frobenius rings in [6]. Let R be a finite commutative Frobenius ring and let $G = \{g_1, g_2, \ldots, g_n\}$ be a group of order n and let $v = \sum_{i=1}^{n} \alpha_{g_i} \in RG$. Define the matrix $\sigma(v) \in M_n(R)$ to be $\sigma(v) = (\alpha_{g_1^{-1} g_j})$ where $i, j \in \{1, \ldots, n\}$. We note that the elements $g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}$ are the elements of the group G in a some given order. We will now describe $\sigma(v)$ for the following group rings RG where $G \in \{C_8 \text{ and } D_{16}\}$.

(i) Let $G = \langle x \mid x^8 = 1 \rangle \cong C_8$. If $v = \sum_{i=0}^{3} \sum_{j=0}^{1} \alpha_{i+4j+1} x^{2i+j} \in RC_8$, then

$$\sigma(v) = \begin{pmatrix} A & B \\ B' & A \end{pmatrix} \tag{3}$$

where $A = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, $B = circ(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$, $B' = circ(\alpha_8, \alpha_5, \alpha_6, \alpha_7)$ and $\alpha_i \in R$.

(ii) Let $G = \langle x, y \mid x^8 = y^2 = 1, x^y = x^{-1} \rangle \cong D_{16}$. If $v = \sum_{i=0}^{7} \sum_{j=0}^{1} \alpha_{1+i+8j} x^i y^j \in RD_{16}$, then

$$\sigma(v) = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} \tag{4}$$

where $A = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8)$, $B = circ(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16})$ and $\alpha_i \in R$.

3 Composite constructions from Group Rings where the orders of the groups are 16 and 8

In this section, we define the 4×4 block matrix by combining the block matrices defined in the previous section. We do this by following the two steps:

(1) take the 2×2 block matrices defined in (4),

(2) take the first row of each matrix in and apply to each the construction defined in (3).

Namely,

$$\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} \to \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1' & A_1 & B_2' & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B_3' & A_3 & B_4' & A_4 \end{pmatrix}, \tag{5}$$

where $A_1 = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4), B_1 = circ(\alpha_5, \alpha_6, \alpha_7, \alpha_8), B_1' = circ(\alpha_8, \alpha_5, \alpha_6, \alpha_7), A_2 = circ(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}), B_2 = circ(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}), B_2' = circ(\alpha_{16}, \alpha_{13}, \alpha_{14}, \alpha_{15})$,
$A_3 = circ(\alpha_9, \alpha_{16}, \alpha_{15}, \alpha_{14}), B_3 = circ(\alpha_{13}, \alpha_{12}, \alpha_{11}, \alpha_{10}), B_3' = circ(\alpha_{10}, \alpha_{13}, \alpha_{12}, \alpha_{11}), A_4 = circ(\alpha_1, \alpha_8, \alpha_7, \alpha_6), B_4 = circ(\alpha_5, \alpha_4, \alpha_3, \alpha_2)$ and $B_4' = circ(\alpha_2, \alpha_5, \alpha_4, \alpha_3)$. We now use the matrix in (5) to define the following result.

Theorem 3.1. *The matrix*

$$G = \left[\begin{array}{c|cccc} & A_1 & B_1 & A_2 & B_2 \\ & B_1' & A_1 & B_2' & A_2 \\ I_{16} & A_3 & B_3 & A_4 & B_4 \\ & B_3' & A_3 & B_4' & A_4 \end{array}\right], \tag{6}$$

where $A_1 = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4), B_1 = circ(\alpha_5, \alpha_6, \alpha_7, \alpha_8), B_1' = circ(\alpha_8, \alpha_5, \alpha_6, \alpha_7), A_2 = circ(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}), B_2 = circ(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}), B_2' = circ(\alpha_{16}, \alpha_{13}, \alpha_{14}, \alpha_{15})$,
$A_3 = circ(\alpha_9, \alpha_{16}, \alpha_{15}, \alpha_{14}), B_3 = circ(\alpha_{13}, \alpha_{12}, \alpha_{11}, \alpha_{10}), B_3' = circ(\alpha_{10}, \alpha_{13}, \alpha_{12}, \alpha_{11}), A_4 = circ(\alpha_1, \alpha_8, \alpha_7, \alpha_6), B_4 = circ(\alpha_5, \alpha_4, \alpha_3, \alpha_2)$ *and* $B_4' = circ(\alpha_2, \alpha_5, \alpha_4, \alpha_3)$, *is the generator matrix of a self-dual code over* R, *if and only if the following equations hold in* R*:*

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_4, \tag{7}$$

$$A_1 B_1' + A_1 B_1 + A_2 B_2' + A_2 B_2 = 0, \tag{8}$$

$$B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_4, \tag{9}$$

$$A_1 A_3 + A_2 A_4 + B_1 B_3 + B_2 B_4 = 0, \tag{10}$$

$$A_1 B_3' + A_2 B_4' + A_3 B_1 + A_4 B_2 = 0, \tag{11}$$

$$A_3B_1' + A_4B_2' + A_1B_3 + A_2B_4 = 0, \tag{12}$$

$$B_1'B_3' + B_2'B_4' + A_1A_3 + A_2A_4 = 0, \tag{13}$$

$$A_3^2 + A_4^2 + B_3^2 + B_4^2 = -I_4, \tag{14}$$

$$A_3B_3' + A_3B_3 + A_4B_4' + A_4B_4 = 0, \tag{15}$$

$$B_3'^2 + B_4'^2 + A_3^2 + A_4^2 = -I_4. \tag{16}$$

Proof. The code generated will be self-dual if and only if GG^T is the zero matrix over R. Let

$$X = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1' & A_1 & B_2' & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B_3' & A_3 & B_4' & A_4 \end{bmatrix},$$

then we have to show that $XX^T = -I_{16}$. Now,

$$XX^T = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1' & A_1 & B_2' & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B_3' & A_3 & B_4' & A_4 \end{bmatrix} \begin{bmatrix} A_1 & B_1' & A_3 & B_3' \\ B_1 & A_1 & B_3 & A_3 \\ A_2 & B_2' & A_4 & B_4' \\ B_2 & A_2 & B_4 & A_4 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix},$$

where

$$X_1 = \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & A_1B_1' + A_1B_1 + A_2B_2' + A_2B_2 \\ A_1B_1' + A_1B_1 + A_2B_2' + A_2B_2 & B_1'^2 + B_2'^2 + A_1^2 + A_2^2 \end{bmatrix},$$

$$X_2 = \begin{bmatrix} A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 & A_1B_3' + A_2B_4' + A_3B_1 + A_4B_2 \\ A_3B_1' + A_4B_2' + A_1B_3 + A_2B_4 & B_1'B_3' + B_2'B_4' + A_1A_3 + A_2A_4 \end{bmatrix},$$

$$X_3 = \begin{bmatrix} A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 & A_3B_1' + A_4B_2' + A_1B_3 + A_2B_4 \\ A_1B_3' + A_2B_4' + A_3B_1 + A_4B_2 & B_1'B_3' + B_2'B_4' + A_1A_3 + A_2A_4 \end{bmatrix},$$

$$X_4 = \begin{bmatrix} A_3^2 + A_4^2 + B_3^2 + B_4^2 & A_3B_3' + A_3B_3 + A_4B_4' + A_4B_4 \\ A_3B_3' + A_3B_3 + A_4B_4' + A_4B_4 & B_3'^2 + B_4'^2 + A_3^2 + A_4^2 \end{bmatrix}.$$

This will equal to $-I_{16}$ only if $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_4, A_1B_1' + A_1B_1 + A_2B_2' + A_2B_2 = 0, B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_4, A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 = 0, A_1B_3' + A_2B_4' + A_3B_1 + A_4B_2 = 0, A_3B_1' + A_4B_2' + A_1B_3 + A_2B_4 = 0, B_1'B_3' + B_2'B_4' + A_1A_3 + A_2A_4 = 0, A_3^2 + A_4^2 + B_3^2 + B_4^2 = -I_4, A_3B_3' + A_3B_3 + A_4B_4' + A_4B_4 = 0$ and $B_3'^2 + B_4'^2 + A_3^2 + A_4^2 = -I_4$. □

3.1 Expanding the search field

Here, we expand the search field in the generator matrix defined in Theorem 3.1 by replacing the elements $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8)$ with $(\alpha_{17}, \alpha_{18}, \alpha_{19}, \alpha_{20}, \alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24})$ where $\alpha_i \in R$, respectively, in one of the sub-matrices and keeping the structure of the generator matrix the same. Namely, the generator matrix in (6) becomes:

$$\left[\begin{array}{c|cc} & A_1\ B_1 & A_2\ B_2 \\ I_{16} & B_1'\ A_1 & B_2'\ A_2 \\ & A_3\ B_3 & A_4\ B_4 \\ & B_3'\ A_3 & B_4'\ A_4 \end{array}\right] \rightarrow \left[\begin{array}{c|cc} & A_1\ B_1 & A_2\ B_2 \\ I_{16} & B_1'\ A_1 & B_2'\ A_2 \\ & A_3\ B_3 & A_{4'}\ B_{4'} \\ & B_3'\ A_3 & B_{4'}'\ A_{4'} \end{array}\right]. \tag{17}$$

Here, $A_4 \mapsto A_{4'}$, $B_4 \mapsto B_{4'}$ and $B_4' \mapsto B_{4'}'$ so that $A_{4'} = circ(\alpha_{17}, \alpha_{24}, \alpha_{23}, \alpha_{22})$, $B_{4'} = circ(\alpha_{21}, \alpha_{20}, \alpha_{19}, \alpha_{18})$ and $B_{4'}' = circ(\alpha_{18}, \alpha_{21}, \alpha_{20}, \alpha_{19})$. We can now state following result:

Theorem 3.2. *The matrix*

$$G = \left[\begin{array}{c|cc} & A_1\ B_1 & A_2\ B_2 \\ I_{16} & B_1'\ A_1 & B_2'\ A_2 \\ & A_3\ B_3 & A_{4'}\ B_{4'} \\ & B_3'\ A_3 & B_{4'}'\ A_{4'} \end{array}\right], \tag{18}$$

where $A_1 = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4), B_1 = circ(\alpha_5, \alpha_6, \alpha_7, \alpha_8), B_1' = circ(\alpha_8, \alpha_5, \alpha_6, \alpha_7), A_2 = circ(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}), B_2 = circ(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}), B_2' = circ(\alpha_{16}, \alpha_{13}, \alpha_{14}, \alpha_{15})$,
$A_3 = circ(\alpha_9, \alpha_{16}, \alpha_{15}, \alpha_{14}), B_3 = circ(\alpha_{13}, \alpha_{12}, \alpha_{11}, \alpha_{10}), B_3' = circ(\alpha_{10}, \alpha_{13}, \alpha_{12}, \alpha_{11}), A_{4'} = circ(\alpha_{17}, \alpha_{24}, \alpha_{23}, \alpha_{22})$, $B_{4'} = circ(\alpha_{21}, \alpha_{20}, \alpha_{19}, \alpha_{18})$ *and* $B_{4'}' = circ(\alpha_{18}, \alpha_{21}, \alpha_{20}, \alpha_{19})$, *is the generator matrix of a self-dual code over* R, *if and only if the following equations hold in* R*:*

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_4, \tag{19}$$

$$A_1 B_1' + A_1 B_1 + A_2 B_2' + A_2 B_2 = 0, \tag{20}$$

$$B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_4, \tag{21}$$

$$A_1 A_3 + A_2 A_{4'} + B_1 B_3 + B_2 B_{4'} = 0, \tag{22}$$

$$A_1 B_3' + A_2 B_{4'}' + A_3 B_1 + A_{4'} B_2 = 0, \tag{23}$$

$$A_3 B_1' + A_{4'} B_2' + A_1 B_3 + A_2 B_{4'} = 0, \tag{24}$$

$$B_1' B_3' + B_2' B_{4'}' + A_1 A_3 + A_2 A_{4'} = 0, \tag{25}$$

$$A_3^2 + A_{4'}^2 + B_3^2 + B_{4'}^2 = -I_4, \tag{26}$$

$$A_3 B_3' + A_3 B_3 + A_{4'} B_{4'}' + A_{4'} B_{4'} = 0, \tag{27}$$

$$B_3'^2 + B_{4'}'^2 + A_3^2 + A_{4'}^2 = -I_4. \tag{28}$$

Proof. The code generated will be self-dual if and only if GG^T is the zero matrix over R. Let

$$X = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1' & A_1 & B_2' & A_2 \\ A_3 & B_3 & A_{4'} & B_{4'} \\ B_3' & A_3 & B_{4'}' & A_{4'} \end{bmatrix},$$

then we have to show that $XX^T = -I_{16}$. Now,

$$XX^T = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1' & A_1 & B_2' & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B_3' & A_3 & B_4' & A_4 \end{bmatrix} \begin{bmatrix} A_1 & B_1' & A_3 & B_3' \\ B_1 & A_1 & B_3 & A_3 \\ A_2 & B_2' & A_{4'} & B_{4'}' \\ B_2 & A_2 & B_{4'} & A_{4'} \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix},$$

where

$$X_1 = \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & A_1B_1' + A_1B_1 + A_2B_2' + A_2B_2 \\ A_1B_1' + A_1B_1 + A_2B_2' + A_2B_2 & B_1'^2 + B_2'^2 + A_1^2 + A_2^2 \end{bmatrix},$$

$$X_2 = \begin{bmatrix} A_1A_3 + A_2A_{4'} + B_1B_3 + B_2B_{4'} & A_1B_3' + A_2B_{4'}' + A_3B_1 + A_{4'}B_2 \\ A_3B_1' + A_{4'}B_2' + A_1B_3 + A_2B_{4'} & B_1'B_3' + B_2'B_{4'}' + A_1A_3 + A_2A_{4'} \end{bmatrix},$$

$$X_3 = \begin{bmatrix} A_1A_3 + A_2A_{4'} + B_1B_3 + B_2B_{4'} & A_3B_1' + A_{4'}B_2' + A_1B_3 + A_2B_{4'} \\ A_1B_3' + A_2B_{4'}' + A_3B_1 + A_{4'}B_2 & B_1'B_3' + B_2'B_{4'}' + A_1A_3 + A_2A_{4'} \end{bmatrix},$$

$$X_4 = \begin{bmatrix} A_3^2 + A_{4'}^2 + B_3^2 + B_{4'}^2 & A_3B_3' + A_3B_3 + A_{4'}B_{4'}' + A_{4'}B_{4'} \\ A_3B_3' + A_3B_3 + A_{4'}B_{4'}' + A_{4'}B_{4'} & B_3'^2 + B_{4'}'^2 + A_3^2 + A_{4'}^2 \end{bmatrix}.$$

This will equal to $-I_{16}$ only if $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_4, A_1B_1' + A_1B_1 + A_2B_2' + A_2B_2 = 0, B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_4, A_1A_3 + A_2A_{4'} + B_1B_3 + B_2B_{4'} = 0, A_1B_3' + A_2B_{4'}' + A_3B_1 + A_{4'}B_2 = 0, A_3B_1' + A_{4'}B_2' + A_1B_3 + A_2B_{4'} = 0, B_1'B_3' + B_2'B_{4'}' + A_1A_3 + A_2A_{4'} = 0, A_3^2 + A_{4'}^2 + B_3^2 + B_{4'}^2 = -I_4, A_3B_3' + A_3B_3 + A_{4'}B_{4'}' + A_{4'}B_{4'} = 0$ and $B_3'^2 + B_{4'}'^2 + A_3^2 + A_{4'}^2 = -I_4$. □

The above result is an extension of Theorem 3.1, the structure of the generator matrix in (18) is the same as in (6) with the difference of an expanded search field. We note that if $R = \mathbb{F}_2$ then there are $2^{16} = 65536$ calculations when using the generator matrix (6) and $2^{24} = 16777216$ calculations when using the generator matrix (18). In other words, we give the generator matrix in Theorem 3.1 more 'freedom' by not letting the submatrices: A_4, B_4 and B_4' be only dependant on the submatrices: A_1, B_1 and B_1'. If the matrix in (6) produces a self-dual code, we can expect the matrix (18) to produce the same code and this will be when the submatrices: $A_{4'}, B_{4'}$ and $B_{4'}'$ of (18) are equal to the submatrices: A_4, B_4 and B_4' of (6).

4 Extremal Self-Dual Codes of Length 64 from Lifts

In this section, we apply Theorems 3.1 and 3.2 over $\mathbb{F}_2$ to search for binary codes with parameters $[38, 16, 8]$ and $[32, 16, 6]$. We then take the Gray images of the codes over $\mathbb{F}_2+u\mathbb{F}_2$ to obtain extremal self-dual codes with parameters $[64, 32, 12]$. Examples of such approach can be found in [10].

There are two possibilities for the weight enumerators of extremal singly-even $[64, 32, 12]_2$ codes ([1]):

$$W_{64,1} = 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \ldots, \ 14 \leq \beta \leq 284,$$

$$W_{64,2} = 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + \ldots, \ 0 \leq \beta \leq 277.$$

With the most updated information, the existence of codes is known for $\beta = 14, 18, 22, 25, 29, 32, 35, 36, 39, 44, 46, 53, 59, 60, 64$ and 74 in $W_{64,1}$ and for $\beta = 0, 1, 2, 4, 5, 6, 8, 9, 10, 12, 13, 14, 16, \ldots, 25, 28, 29, 30, 32, 33, 34, 36, 37, 38, 40, 41, 42, 44, 45, 48, 50, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120$ and 184 in $W_{64,2}$.

We now apply Theorem 3.1 to search for binary codes with parameters $[38, 16, 8]$ and $[32, 16, 6]$. The results are summarised below.

Table 1: Codes of length 32 via Theorem 3.1

Code	A_1	B_1	A_2	B_2	$\lvert Aut(C)\rvert$	Type
C_1	$(0,0,0,0)$	$(0,0,1,1)$	$(0,0,1,1)$	$(0,1,1,1)$	$2^{15} \cdot 3^2 \cdot 5 \cdot 7$	$[32,16,8]_{II}$
C_2	$(0,0,0,1)$	$(0,0,1,1)$	$(1,0,0,1)$	$(1,1,1,1)$	$2^{15} \cdot 3^2$	$[32,16,8]_{I}$
C_3	$(0,0,0,1)$	$(0,1,0,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$2^5 \cdot 3 \cdot 5 \cdot 31$	$[32,16,8]_{II}$
C_4	$(0,0,1,1)$	$(0,0,1,1)$	$(0,1,0,1)$	$(0,1,1,1)$	2^5	$[32,16,6]_{I}$

We now lift all four codes and summarise the results in a table. We include codes of length 64 with different values of beta and different orders of automorphism groups. If a code with the same parameters (the same value of beta and the same order of automorphism groups) appears, it means that they were used to produce different and new codes of length 68 in the later section of the paper.

Table 2: Extremal self-dual codes of length 64 obtained from lifts of C_1, C_2, C_3 and C_4

Code		A_1	B_1	A_2	B_2	$\lvert Aut(C)\rvert$	$W_{64,2}$
I_1	C_1	$(u,0,0,u)$	$(u,u,1,u+1)$	$(u,u,1,1)$	$(u,1,1,u+1)$	2^5	$\beta=16$
I_2	C_1	$(u,u,u,0)$	$(u,u,1,u+1)$	$(u,0,1,u+1)$	$(u,1,1,u+1)$	2^6	$\beta=16$
I_3	C_1	$(0,0,0,a)$	$(0,0,1,a+1)$	$(u,0,1,u+1)$	$(u,1,1,u+1)$	2^7	$\beta=16$
I_4	C_1	$(0,0,u,u)$	$(0,0,1,u+1)$	$(u,u,1,1)$	$(u,1,1,u+1)$	2^5	$\beta=32$
I_5	C_1	$(0,0,0,u)$	$(0,u,1,1)$	$(0,u,1,u+1)$	$(0,1,1,u+1)$	2^5	$\beta=48$
I_6	C_2	$(u,u,0,1)$	$(u,u,u+1,u+1)$	$(1,u,u,u+1)$	$(1,1,u+1,u+1)$	2^5	$\beta=16$
I_7	C_2	$(u,u,0,1)$	$(u,u,1,1)$	$(1,0,0,u+1)$	$(1,1,u+1,u+1)$	2^5	$\beta=32$
I_8	C_3	$(0,0,u,1)$	$(0,1,0,1)$	$(u,0,1,1)$	$(u,0,u+1,1)$	2^5	$\beta=0$
I_9	C_3	$(0,u,u,1)$	$(0,1,0,1)$	$(0,0,1,1)$	$(0,u,u+1,u+1)$	2^5	$\beta=16$
I_{10}	C_3	$(u,u,0,1)$	$(u,1,u,1)$	$(0,0,1,u+1)$	$(0,u,u+1,1)$	2^5	$\beta=32$
I_{11}	C_4	$(u,u,1,1)$	$(u,u,1,u+1)$	$(u,1,0,u+1)$	$(u,u+1,1,1)$	2^5	$\beta=0$
I_{12}	C_4	$(u,u,1,1)$	$(u,0,1,1)$	$(0,1,u,u+1)$	$(0,u+1,1,1)$	2^5	$\beta=0$
I_{13}	C_4	$(0,0,1,1)$	$(0,u,1,1)$	$(0,1,u,u+1)$	$(0,u+1,1,1)$	2^5	$\beta=0$
I_{14}	C_4	$(0,0,1,1)$	$(0,0,1,u+1)$	$(u,1,0,u+1)$	$(u,u+1,1,1)$	2^5	$\beta=0$
I_{15}	C_4	$(u,0,1,1)$	$(u,u,1,1)$	$(u,1,u,1)$	$(u,u+1,u+1,1)$	2^5	$\beta=16$
I_{16}	C_4	$(0,u,1,u+1)$	$(0,0,1,u+1)$	$(u,1,u,1)$	$(u,1,u,u+1)$	2^5	$\beta=32$
I_{17}	C_4	$(u,0,1,u+1)$	$(u,0,1,1)$	$(u,1,0,u+1)$	$(u,1,1,u+1)$	2^5	$\beta=48$

Now we search for binary self-dual codes with parameters $[32,16,8]$ and $[32,16,6]$, by applying the generator matrix defined in (18), in other words, we apply Theorem 3.1 with an extended search field. We were able to find the same codes as in Table 1 as expected, plus some other ones with different automorphism groups. These are listed in the table below. We use a slightly different table display to the tables before, to enable us to fit the results.

Table 3: Codes of length 32 via Theorem 3.2

	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}
A_1	$(0,0,0,1)$	$(0,0,0,1)$	$(0,0,0,1)$	$(0,0,0,1)$	$(0,0,0,1)$	$(0,0,0,1)$	$(0,0,0,1)$
B_1	$(0,0,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$(0,1,0,1)$
A_2	$(0,0,1,1)$	$(0,1,0,1)$	$(0,0,0,0)$	$(0,0,0,0)$	$(0,0,0,0)$	$(0,1,0,1)$	$(0,0,1,1)$
B_2	$(0,1,0,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$	$(0,0,1,1)$
$A_{4'}$	$(1,0,0,1)$	$(1,0,0,1)$	$(0,1,1,0)$	$(1,0,0,1)$	$(1,0,0,1)$	$(1,0,0,1)$	$(0,1,0,1)$
$B_{4'}$	$(0,1,0,0)$	$(1,0,1,1)$	$(1,0,1,1)$	$(0,1,0,0)$	$(1,0,1,1)$	$(1,0,1,1)$	$(1,0,1,1)$
$\lvert Aut(C)\rvert$	$2^9\cdot 3^2\cdot 5$	$2^{12}\cdot 3\cdot 7$	2^6	$2^9\cdot 3^2\cdot 5$	2^{11}	$2^{12}\cdot 3\cdot 7$	2^4
Type	$[32,16,8]_{II}$	$[32,16,6]_I$	$[32,16,6]_I$	$[32,16,6]_I$	$[32,16,6]_I$	$[32,16,6]_I$	$[32,16,6]_I$

We now take the Gray images of the above codes over $\mathbb{F}_2+u\mathbb{F}_2$ to obtain extremal self-dual codes with parameters $[64,32,12]$. The only codes that have actually worked in that case were: C_7, C_9 and C_{10}. The results are summarised in the tables below.

Table 4: Extremal self-dual codes of length 64 obtained from lifts of C_7

	I_{18}	I_{21}	I_{22}	I_{23}	I_{24}
A_1	$(u,u,0,1)$	$(u,0,0,1)$	$(u,u,0,1)$	$(u,u,0,1)$	$(u,0,0,1)$
B_1	$(u,0,1,u+1)$	$(0,u,1,u+1)$	$(0,u,1,u+1)$	$(u,u,1,1)$	$(u,0,1,u+1)$
A_2	$(u,0,u,0)$	(u,u,u,u)	(u,u,u,u)	$(u,u,0,0)$	$(0,u,0,u)$
B_2	$(u,0,1,1)$	$(u,u,1,u+1)$	$(u,u,1,u+1)$	$(u,u,1,u+1)$	$(0,0,1,u+1)$
$A_{4'}$	$(0,1,u+1,u)$	$(u,1,u+1,0)$	$(u,1,u+1,0)$	$(u,1,1,u)$	$(0,1,u+1,u)$
$B_{4'}$	$(u+1,u,1,1)$	$(1,0,u+1,1)$	$(1,0,u+1,u+1)$	$(u+1,u,1,1)$	$(u+1,u,1,1)$
$\lvert Aut(C)\rvert$	2^4	2^6	2^5	2^4	2^5
Type	$\beta=0$	$\beta=0$	$\beta=4$	$\beta=16$	$\beta=36$

Table 5: Extremal self-dual codes of length 64 obtained from lifts of C_9

	I_{25}	I_{26}	I_{27}	I_{28}
A_1	$(u,u,0,1)$	$(u,u,0,1)$	$(u,0,0,1)$	$(u,0,0,1)$
B_1	$(u,u,1,1)$	$(u,0,1,u+1)$	$(u,0,1,u+1)$	$(0,u,1,u+1)$
A_2	$(0,u,u,u)$	$(u,0,u,u)$	$(u,u,u,0)$	$(0,0,0,u)$
B_2	$(0,0,1,u+1)$	$(u,0,1,1)$	$(u,u,1,u+1)$	$(0,u,1,1)$
$A_{4'}$	$(1,u,u,1)$	$(1,0,u,u+1)$	$(u+1,u,0,1)$	$(u+1,0,u,1)$
$B_{4'}$	$(u+1,0,1,u+1)$	$(u+1,0,1,u+1)$	$(1,u,u+1,u+1)$	$(u+1,0,1,1)$
$\lvert Aut(C)\rvert$	2^4	2^4	2^5	2^4
Type	$\beta=12$	$\beta=20$	$\beta=20$	$\beta=32$

Table 6: Extremal self-dual codes of length 64 obtained from lifts of C_{10}

	I_{29}	I_{30}
A_1	$(u,0,0,1)$	$(u,u,0,1)$
B_1	$(u,0,1,u+1)$	$(u,0,1,u+1)$
A_2	$(u,1,0,1)$	$(u,1,0,1)$
B_2	$(u,u,u+1,1)$	$(u,u,1,u+1)$
$A_{4'}$	$(1,0,u,u+1)$	$(u+1,u,0,1)$
$B_{4'}$	$(u+1,0,1,1)$	$(u+1,0,1,u+1)$
$\lvert Aut(C)\rvert$	2^4	2^4
Type	$\beta=16$	$\beta=36$

5 New Extremal Binary Self-Dual Codes of Length 68 via Extensions and Neighbors

In the sequel, let R be a commutative Frobenius ring with identity. Here, we define a well known extension method ([8]) which we then apply to the codes of length 64 tabulated in the previous section, to search for new extremal binary self dual codes with parameters $[68, 34, 12]_2$. The weight enumerator of a self-dual $[68, 34, 12]_2$ code is in one of the following forms ([11]):

$$W_{68,1} = 1 + (442 + 4\beta)y^{12} + (10864 - 8\beta)y^{14} + \dots,$$
$$W_{68,2} = 1 + (442 + 4\beta)y^{12} + (14960 - 8\beta - 256\gamma)y^{14} + \dots\ ,$$

where β and γ are parameters and $0 \le \gamma \le 0$. The existence of the codes in $W_{68,2}$ is known for the following parameters (see [3, 12]):

$\gamma = 0,\ \beta = 0, 7, 11, 14, 17, 21, 22, 28, 33, 35, 42, \dots, 158, 161, 165,$
$175, 187, 189, 203, 209, 221, 231, 255, 303$ or
$\beta \in \{2m | m = 17, 20, 102, 110, 119, 136, 165 \text{ or } 80 \le m \le 99\}$;
$\gamma = 1,\ \beta = 49, 51, 53, 55, 57, \dots, 160$ or $\beta \in \{2m | m = 22, \dots, 29, 81, \dots, 99\}$;
$\gamma = 2,\ \beta = 65, 69, 71, 73, 75, 77, 79, 81, 141, 159, 161, 163, 166, 167, 168, 169, 171, 173, 206, 208$
or $\beta \in \{2m | 29 \le m \le 68, 70 \le m \le 100\}$ or $\beta \in \{2m + 1 | 41 \le m \le 69, 71 \le m \le 77\}$;
$\gamma = 3,\ \beta \in \{2m + 1 | m = 43, 44, 47, \dots, 77, 79, 80, 81, 83, 87, 88, 96\}$ or
$\beta \in \{2m | m = 40, \dots, 92, 94, 95, 97, 98, 101, 102\}$;
$\gamma = 4,\ \beta = 103, 105, 107, 109, 113, 115, 117, 119, 121, 129, 139, 141, 143, 145, 149, 157,$
$159, 161, 175, 191$ or
$\beta \in \{2m | m = 43, 45, 47, 48, 49, 51, 52, 54, 55, 56, 58, 60, \dots, 90, 92, 93, 97, 98, 100\}$;
$\gamma = 5$ with $\beta \in \{m | m = 113, 116, \dots, 182, 187, 189, 191, 193\}$
$\gamma = 6$ with $\beta \in \{2m | m = 69, 77, 78, 79, 81, 88\}$
$\gamma = 7$ with $\beta \in \{7m | m = 14, \dots, 39, 42\}$.

Theorem 5.1. *([8]) Let C be a self-dual code of length n over R and $G = (r_i)$ be a $k \times n$ generator matrix for C, where r_i is the i-th row of G, $1 \le i \le k$. Let c be a unit in R such that $c^2 = -1$ and X be a vector in S^n with $\langle X, X\rangle = -1$. Let $y_i = \langle r_i, X\rangle$ for $1 \le i \le k$. The following matrix*

$$\left[\begin{array}{cc|c} 1 & 0 & X \\ \hline y_1 & cy_1 & r_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & r_k \end{array}\right],$$

generates a self-dual code D over R of length $n + 2$.

Theorem 5.1 is applied to the $\phi_{\mathbb{F}_2+u\mathbb{F}_2}$-images of the codes in tables 2, 4, 5 and 6. The results are tabulated in table 7, where $1 + u$ in $\mathbb{F}_2 + u\mathbb{F}_2$ is denoted as 3.

Table 7: New codes of length 68 from Theorem 5.1

$C_{68,i}$	Code	$(x_{17}, x_{18}, \ldots, x_{32})$	c	γ	β *in* $W_{64,2}$
$C_{68,1}$	I_{13}	$(3,1,0,u,3,0,0,0,3,u,1,u,3,3,0,1,3,1,u,u,u,3,0,0,3,u,1,1,1,3,0,1)$	1	**0**	**36**
$C_{68,2}$	I_{11}	$(u,1,0,0,0,u,0,u,1,0,0,3,1,u,0,3,3,1,0,u,3,u,u,1,0,3,1,3,3,1,1,0)$	1	**1**	**30**
$C_{68,3}$	I_{12}	$(3,0,0,3,1,1,u,3,1,3,u,0,u,3,1,1,3,0,3,0,0,0,0,1,0,1,3,3,3,0,u,u)$	3	**1**	**40**
$C_{68,4}$	I_{11}	$(3,1,3,1,3,u,u,1,u,0,1,u,0,0,3,1,0,u,0,u,3,0,u,1,u,1,3,0,u,1,0,1)$	3	**1**	**42**
$C_{68,5}$	I_{18}	$(u,1,0,3,0,0,0,3,1,0,0,0,0,1,3,3,1,3,1,3,3,3,1,0,u,1,u,3,3,3,0,3)$	1	**1**	**47**
$C_{68,6}$	I_{21}	$(0,1,1,u,1,1,u,u,1,1,1,u,0,1,1,3,u,3,3,1,3,3,1,1,1,1,0,3,0,3,3,3)$	1	**2**	**63**
$C_{68,7}$	I_{14}	$(3,3,1,0,3,1,0,3,3,3,u,u,0,u,u,u,3,u,1,0,1,u,0,3,3,1,3,3,3,0,1,1)$	1	**3**	**76**
$C_{68,8}$	I_{18}	$(1,1,1,u,1,u,u,0,1,3,0,1,u,1,3,u,3,1,1,1,3,u,3,0,3,1,u,0,1,0,3,0)$	3	**4**	**88**
$C_{68,9}$	I_{18}	$(3,3,1,u,1,u,u,u,1,1,u,1,0,1,1,0,1,3,1,1,1,0,1,u,3,1,0,u,3,u,3,0)$	3	4	90
$C_{68,10}$	I_{18}	$(1,3,1,0,1,u,0,u,3,1,0,3,u,3,1,0,3,1,1,1,3,0,1,0,3,3,0,u,1,0,3,0)$	1	**4**	**106**
$C_{68,11}$	I_{18}	$(1,3,3,u,3,u,u,0,1,1,0,1,0,3,1,0,3,1,3,1,3,0,3,0,1,3,0,u,1,0,1,0)$	1	**4**	**118**
$C_{68,12}$	I_{18}	$(1,1,1,u,1,0,u,u,1,1,u,1,0,3,1,0,1,3,3,1,3,u,1,u,1,1,0,0,1,u,3,0)$	3	**6**	**118**

Two self-dual binary codes of length $2k$ are said to be neighbors if their intersection has dimension $k-1$. Let $x \in \mathbb{F}_2^n - C$ then $D = \left\langle \langle x \rangle^{\perp} \cap C, x \right\rangle$ is a neighbor of C. We consider the standard form of C to reduce the search field considerably from 2^{68} to 2^{34}. Without loss of generality the first 34 entries of x are set to be 0, the rest of the vectors are listed in Table 8. As neighbors of the codes in Table 7 we obtain seventeen new codes including the ones with rare parameter $\gamma = 6$ in $W_{68,2}$, which are listed in Table 8. All the codes have an automorphism group of order 2.

Table 8: New codes of length 68 with as neighbors

$\mathcal{N}_{68,i}$	$\mathcal{C}_{68,i}$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
$\mathcal{N}_{68,1}$	$\mathcal{C}_{68,9}$	(11000000001111101110001010100011101)	3	91
$\mathcal{N}_{68,2}$	$\mathcal{C}_{68,8}$	(10111100101110111011010100100010101)	4	95
$\mathcal{N}_{68,3}$	$\mathcal{C}_{68,9}$	(10000110001001100110101000110101111)	4	97
$\mathcal{N}_{68,4}$	$\mathcal{C}_{68,9}$	(11111101100011000100001110011001110)	4	99
$\mathcal{N}_{68,5}$	$\mathcal{C}_{68,8}$	(00110011001100011100100010101001111)	4	101
$\mathcal{N}_{68,6}$	$\mathcal{C}_{68,9}$	(11100111110101001001101101010011101)	4	111
$\mathcal{N}_{68,7}$	$\mathcal{C}_{68,9}$	(11101111000100011000111000010001101)	4	123
$\mathcal{N}_{68,8}$	$\mathcal{C}_{68,12}$	(10001110111100001111101100111010011)	5	107
$\mathcal{N}_{68,9}$	$\mathcal{C}_{68,12}$	(11001111001011110110100110100110011)	5	115
$\mathcal{N}_{68,10}$	$\mathcal{C}_{68,12}$	(01111000001111000001101011111010011)	6	125
$\mathcal{N}_{68,11}$	$\mathcal{C}_{68,12}$	(00011010011101011111111100000100110)	6	126
$\mathcal{N}_{68,12}$	$\mathcal{C}_{68,12}$	(01110110110110011011011001000111110)	6	127
$\mathcal{N}_{68,13}$	$\mathcal{C}_{68,12}$	(10111000111101110100001111111011101)	6	128
$\mathcal{N}_{68,14}$	$\mathcal{C}_{68,12}$	(01101110011111010011110110010111110)	6	129
$\mathcal{N}_{68,15}$	$\mathcal{C}_{68,12}$	(00101110010000111101101111000101101)	6	130
$\mathcal{N}_{68,16}$	$\mathcal{C}_{68,12}$	(01010111011100101000110111111100101)	6	131
$\mathcal{N}_{68,17}$	$\mathcal{C}_{68,12}$	(01100100010011110011110100100011111)	6	132

6 Conclusion

In this work, we extended the methods used in [4], to produce a composite construction from group rings, where the orders of the groups are 16 and 8. The composite construction has been amended by expanding the search field. Both, the composite construction and its amended version, together with $\mathbb{F}_2 + u\mathbb{F}_2$-lifts, extension and neighbor methods are used to search for extremal binary self-dual codes of length 68. In particular, we construct the following unknown $W_{64,2}$ codes:

$$
\begin{aligned}
&(\gamma = 0,\ \beta = \{36\}),\\
&(\gamma = 1,\ \beta = \{30, 40, 42, 47\}),\\
&(\gamma = 2,\ \beta = \{63\}),\\
&(\gamma = 3,\ \beta = \{76, 91\}),\\
&(\gamma = 4,\ \beta = \{88, 95, 97, 99, 101, 106, 111, 118, 123\}),\\
&(\gamma = 5,\ \beta = \{107, 115\}),\\
&(\gamma = 6,\ \beta = \{118, 125, 126, 127, 128, 129, 130, 131, 132\}).
\end{aligned}
$$

The binary generator matrices of the codes are available online at [5].

A suggestion for further work would be to consider group rings, where the orders of the groups are higher than 16. This would lead to more composite constructions. Although, this would also lead to expanding the search field which would require a huge number of calculations.

References

[1] J.H. Conway, N.J.A. Solane, "A new upper bound on the minimal distance of self-dual codes", IEEE Trans. Inform. Theory, Vol. 36, 6, pp. 1319-1333, 1990.

[2] S.T. Dougherty, P. Gaborit, M. Harada, P. Sole, "Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$", IEEE Trans. Inform. Theory, Vol. 45, pp. 32-45, 1999.

[3] S.T. Dougherty, J. Gildea, A. Kaya, "Quarduple Bordered Constructions of Self-Dual Codes from Group Rings over Frobenius Rings", Cryptogr. Commun., `https://doi.org/10.1007/s12095-019-00380-8`, 2019.

[4] S. T. Dougherty, J. Gildea, A. Korban, A. Kaya, "Composite Constructions of Self-Dual Codes from Group Rings and New Extremal Self-Dual Binary Codes of Length 68", Advances in Mathematics of Communications, doi: 10.3934/amc.2020037, 2019.

[5] S. T. Dougherty, J. Gildea, A. Korban and A. Kaya "Binary generator matrices for extremal binary self-dual codes of length 68", available online at `http://abidinkaya.wixsite.com/math/adrian2`.

[6] S.T. Dougherty, J. Gildea, R. Taylor and A. Tylshchak, "Group Rings, G-Codes and Constructions of Self-Dual and Formally Self-Dual Codes", Des., Codes and Cryptog., Designs, Vol. 86, no. 9, pp. 2115-2138, 2018.

[7] S.T. Dougherty, T.A. Gulliver, M. Harada, "Extremal binary self dual codes", IEEE Trans. Inform. Theory, Vol. 43, pp. 2036-2047, 1997.

[8] S.T. Dougherty, J. L. Kim, H. Kulosman and H. Liu, "Self-Dual Codes over Commutative Frobenius rings", Finite Fields and Applications, Vol. 16, No. 1, pp. 14-26, 2010.

[9] T. Hurley, "Group Rings and Rings of Matrices", Int. Jour. Pure and Appl. Math, Vol. 31, no. 3, pp. 319-335, 2006.

[10] S. Karadeniz, B. Yildiz, N. Aydin, "Extremal Binary Self-Dual Codes of Lengths 64 and 66 from Four-Circulant Constructions over $\mathbb{F}_2 + u\mathbb{F}_2$", Filomat 28:5 (2014), pp. 937-945.

[11] E.M. Rains, "Shadow Bounds for Self-Dual Codes", IEEE Trans. Inf. Theory, Vol. 44, pp. 134-139, 1998.

[12] A. Kaya, B. Yildiz, "Various constructions for self-dual codes over rings and new binary self-dual codes", Discrete Mathematics, Vol. 339, Issue 2, pp. 460-469, 2016.